Un conjunto de vulnerabilidades críticas en el software de base de datos de Sybase de SAP, puede brindar a los hackers no privilegiados un control completo sobre una base de datos específica e incluso, en el sistema operativo subyacente en algunos escenarios.

Las seis vulnerabilidades, reveladas por la compañía de seguridad cibernética Trustwave, residen en Sybase Adaptive Server Enterprise (ASE), un software de administración de bases de datos relacionales orientado a aplicaciones basadas en transacciones.

La compañía de seguridad dijo que los problemas, tanto específicos del sistema operativo como de la plataforma en su conjunto, se descubrieron durante una prueba de seguridad del producto, uno de los cuales tiene una calificación CVSS de 9.1.

Identificada como CVE-2020-6248, la vulnerabilidad más grave permite la ejecución de código arbitrario al realizar copias de seguridad de la base de datos, lo que permite que un atacante active la ejecución de comandos maliciosos.

> *«Durante las operaciones de respaldo de la base de datos, no existen controles de seguridad para sobrescribir archivos de configuración críticos. Eso significa que cualquiera que pueda ejecutar el comando DUMP puede realizar tareas muy peligrosas»,* dijeron los investigadores.

Una segunda vulnerabilidad, rastreada como CVE-2020-6252, se refiere a ASE Cockpit, una consola administrativa basada en la web, utilizada para monitorear el estado y disponibilidad de los servidores ASE. Al afectar solo las instalaciones de Windows ASE 16, la falla permite a un mal actor acceder a una red local para capturar credenciales de cuenta de usuario, sobrescribir archivos del sistema operativo e incluso ejecutar código malicioso con privilegios de LocalSystem.

Por otro lado, los defectos CVE-2020-6241 y CVE-2020-6253, permiten que un usuario autenticado ejecute consultas de bases de datos diseñadas para elevar sus privilegios mediante inyección SQL, lo que permite a un usuario sin privilegios especiales obtener

acceso de administrador de la base de datos.

En el último caso, un volcado de la base de datos ASE controlado por el atacante se altera con datos maliciosos antes de cargarlo en un servidor ASE de destino.

Una quinta vulnerabilidad, CVE-2020-6243, es aprovechable cuando el servidor no realiza las verificaciones necesarias para un usuario autenticado mientras ejecuta un procedimiento almacenado («dummy_esp»), lo que permite a los usuarios de Windows ejecutar código arbitrario y eliminar datos en el servidor ASE.

Finalmente, CVE-2020-6250, implica la divulgación de información en sistemas Linux en los que un atacante autenticado puede leer las contraseñas de administrador del sistema desde los registros de instalación.

> *«Los registros solo se pueden leer en la cuenta de SAP, pero cuando se unen con algún otro problema que permita el acceso al sistema de archivos, comprometerá completamente el ASE de SAP»,* agregaron los investigadores.

Después de que Trustwave revelara de forma responsable los hallazgos a Sybase, SAP abordó los problemas con un parche que se lanzó el pasado 12 de mayo.

> *«Las organizaciones a menudo almacenan sus datos más críticos en bases de datos, que, a su vez, a menudo se exponen necesariamente en personas no confiables o expuestas públicamente»,* dijo Trustwave.
>
> *«Esto hace que las vulnerabilidades como estas sean esenciales para abordar y probar rápidamente, ya que no solo amenazan los datos en la base de datos, sino potencialmente el host completo en el que se está ejecutando».*

Además de estas seis vulnerabilidades en Adaptive Server, SAP también lanzó parches de seguridad críticos para el servidor de aplicaciones ABAP, Business Client, BusinessObjects, Master Data Governance, Plant Connectivity, NetWeaver y el software SAP Identity Management como parte de su lanzamiento de parches de mayo de 2020.